



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/606,432	06/25/2003	Terence Spies	ID-8	6320

36532 7590 10/04/2007
G. VICTOR TREYZ
FLOOD BUILDING
870 MARKET STREET, SUITE 984
SAN FRANCISCO, CA 94102

EXAMINER

SANDOVAL, KRISTIN D

ART UNIT	PAPER NUMBER
----------	--------------

2132

MAIL DATE	DELIVERY MODE
-----------	---------------

10/04/2007

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/606,432	Applicant(s) SPIES ET AL.	
	Examiner Kristin D. Sandoval	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 09 July 2007.
 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
 5) ☐ Claim(s) _____ is/are allowed.
 6) ☒ Claim(s) 1-28 is/are rejected.
 7) ☐ Claim(s) _____ is/are objected to.
 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
 10) ☒ The drawing(s) filed on 02 February 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152:

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 a) ☐ All b) ☐ Some * c) ☐ None of:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
 * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-28 are pending.

Claim Rejections - 35 USC § 112

2. Amendments and arguments with regard to the previous 112 rejections are accepted and persuasive. The previous 112 rejections are withdrawn.

Response to Arguments

3. Applicant's arguments filed July 9, 2007 have been fully considered but they are not persuasive.

Applicant argues that Slick fails to teach use of an outer layer of message encryption having an associated outer-layer public key to encrypt the inner-layer public key. The examiner respectfully disagrees. Slick discloses an outer-layer of message encryption having an associated outer-layer user public key used to encrypt an inner-layer printer public key and since the printer public key is a key encrypted by the user's public key it represents an inner layer since it's inside relative to the user's public key, thus making the user's public key the outer layer public key associated with the outer layer encryption (10:12-45).

Applicant further argues that Slick fails to disclose an inner layer of message encryption that has an associated inner-layer public key or use of an outer layer private key or inner layer private key. The examiner respectfully disagrees. Slick discloses an inner layer of message encryption that has an associated inner layer printer public key since the printer public key encrypts the symmetric key that encrypts the message, thus making it an inner layer of message encryption since it occurs inside the user's outer layer public key encryption (10:12-45). An associated user private key and printer public key are used in decrypting the message (10:12-45).

Art Unit: 2132

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, it would have been obvious to combine the known technique of identity based encryption as disclosed in Boneh to improve the security of the invention of Boneh.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

4. Claims 1, 2, 4, 5, 6-9, 13, 16, 18, 21-23, 24-28 rejected under 35 U.S.C. 103(a) as being unpatentable over Slick et al. (Slick), U.S. Patent No. 7,003,667 in view of Boneh et al. (Boneh), U.S. Patent No. 7,113,594.

As per claims 1 and 2:

Slick substantially teaches a method comprising:

at the sender, encrypting the message using at least two layers of encryption by using an inner layer of message encryption having an associated inner-layer public key to encrypt the message data and by using an outer layer of message encryption having an associated outer-layer public key to encrypt the inner-layer public key without using a symmetric key; sending the encrypted message to the recipient; and at the recipient, decrypting the encrypted message using an outer-layer private key corresponding to the outer-layer public key and using an inner-layer

Art Unit: 2132

private key corresponding to the inner layer public key (9:27-10:45, 11:20-28, 11:42-64 wherein it would have been obvious to combine the one embodiment of Slick that uses a public key to encrypt the public key that encrypts the symmetric key with the embodiment that encrypts the message using the public key and then encrypting the public key encrypted message again utilizing the first embodiment as suggested by Slick (11:64-67). Since encrypting the message twice with a public key utilizes a lot of system resources, encrypting only the key saves resources while ensuring security (11:67-12:7).

As per claim 4:

Slick substantially teaches a method further comprising:

sending the encrypted message to the recipient comprises sending the encrypted inner-layer public key to the recipient with the encrypted message, and wherein decrypting the encrypted message at the recipient further comprises using the outer-layer private key to decrypt the encrypted inner-layer public key to produce an unencrypted version of the inner-layer public key at the recipient (1:39-58).

As per claim 5:

Slick further teaches a method wherein encrypting the message comprises encrypting the message using at least three layers of encryption and wherein the outer layer is not an outermost layer (10:46-11:28 wherein three keys equals three layers but the third is not the outermost layer since a signed hash can also be appended).

As per claims 6-8, 21-23 and 24-26:

Slick teaches a method comprising:

Art Unit: 2132

encrypting the message by performing at least an inner layer of encryption and an outer layer of encryption at the sender, wherein: performing the inner layer of encryption includes encrypting the message data M using a symmetric key S to produce encrypted message data Ms and encrypting the symmetric key S using an public key QG associated with the inner layer of encryption to produce an encrypted symmetric message key SQG, and performing the outer layer of encryption includes encrypting at least the public key QG using an public key QL, wherein the public key QL is less sensitive than the public key QG; and sending at least the encrypted message data Ms, the encrypted symmetric message key SQG, the public key QL, the encrypted key QGQL and the encrypted public key QG to the recipient (9:27-10:45, 11:4-28).

As per claim 9:

Slick teaches a method further comprising:

using the outer-layer private key to decrypt the inner-layer public key that has been encrypted using the outer-layer public key; using inner-layer private key to decrypt the symmetric key that has been encrypted using the inner-layer public key; and using the symmetric key that has been decrypted using the inner-layer private key to decrypt the message data that was encrypted using the symmetric key (12:7-51).

As per claim 13:

Slick further teaches a method wherein at least one of the data attributes has an associated sensitivity level and wherein encrypting the message data comprises using the sensitivity level in determining how to encrypt the message (1:14-22).

As per claims 15 and 16:

Art Unit: 2132

Boneh further teaches a method wherein encrypting an email message comprises utilizing an age based policy (29:55-63).

As per claims 27 and 28:

Boneh further teaches a public key based on a recipient's email address (2:45-62).

Slick fails to disclose the key and encryption being IBE, however, Boneh discloses utilizing IBE as an asymmetric encryption scheme (abstract). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to make the keys be identity based as suggested by Slick, in order to ensure the intended recipients receive the printout or fax, having keys based on their identity would ensure that only they could read it and only printers or fax machines associated with them could decrypt the information (Slick, 1:14-58).

5. Claims 10, 11 and 18-20 rejected under 35 U.S.C. 103(a) as being unpatentable over Slick in view of Boneh as applied to claim 1 above, and further in view of Van Oorschot et al. (Van Oorschot), U.S. Patent No. 5,850,443.

As per claims 10 and 18-20:

Slick and Boneh fail to disclose varying sensitivity levels of the multiple encryption keys and the keys having overlapping components. However, Van Oorschot discloses a method wherein varying strengths of multiple encryption keys are used and the keys are concatenated together, therefore each key shares the same components with all the others (4:16-56).

It would have been obvious to utilize varying encryption key strengths along with overlapping components because it allows multiple parties to communicate over varying trust environments and to share cryptographic keys (Van Oorschot, 1:66-2:13).

As per claim 11:

Art Unit: 2132

Slick further teaches a method wherein encrypting the message comprises encrypting the message using at least three layers of encryption and wherein the outer layer is not an outermost layer (10:46-11:28 wherein three keys equals three layers but the third is not the outermost layer since a signed hash can also be appended).

6. Claim 17 rejected under 35 U.S.C. 103(a) as being unpatentable over Slick in view of Boneh as applied to claim 1 above, and further in view of Lord et al. (Lord), U.S. Patent No. 7,131,003.

With regard to claim 17, Slick and Boneh fail to teach the encrypted message comprising an instant message. However, Lord discloses a method of encrypting instant messages (2:35-49). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to increase the security of instant messages as suggested by Lord (1:41-62).

Allowable Subject Matter

7. Claim 3 objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

Art Unit: 2132

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kristin D. Sandoval whose telephone number is 571-272-7958. The examiner can normally be reached on Monday - Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

KDS
KDS

Kristin D Sandoval
Examiner
Art Unit 2132


GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100